BLOCKING OF WEBSITES IN INDIA: LAWS AND PRACTICES

Dr. P.K. Pandey*
Shreya Pandey**

Section 69A of the Information Technology Act, 2000 is a narrowly drawn provision with several safeguards.

-Supreme Court of India[1]

***Abstract*:** The innovative character of human beings has helped a lot in achieving many things required for their easy and comfortable life. The human beings, through their hard labour and energized work, have invented such a platform where the whole world looks like a village in which things are accessible within few minutes which are the result of our ongoing hard work. But, at the same time it has to keep in mind that these achievements have to be utilized cautiously otherwise the consequences may be disastrous. In other achievements, the access of information technology is very vital for development of not only this generation rather it has efficiency to do many things for future generations also. It is the result of information technology that today we are able to have connections from items located at other planets also. For proper regulation of information technology equipped society, the Indian Parliament has enacted Information Technology Act. Under the provisions of this Act, the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 has been made by the Central Government.

***Keywords*:** Information Technology, Website, Law.

Introduction:

The information technology, on one hand, has provided many things which have made our life comfortable through providing quick, efficient and prompt access to the whole world but on other hand it may, if intentionally used for misfeasance, result in varied nature of devastating loss not only to single person rather to humanity also. It is well accepted fact that the development and rapid increase in the use of information technology including computer, mobile phone and internet has given rise to new forms of offences and thus the effective regulatory mechanisms to control and root-out such ill-intended activities are need of hour. With the help of information technology, the information may be posted from any place of the world and any person having internet connection through mobile phones or computers may access and accordingly act or react. It is well known fact that people, on the basis of religion, are coming into touch with terroristic groups through various websites and they are being brain-washed and trained to fight against humanity. Not only this, as mentioned in the Statement of Objects and Reasons of Bill which introduced the Information Technology (Amendment) Act, 2008, 'publishing sexually explicit materials in electronic form, video voyeurism and breach of confidentiality and leakage of

***Assistant Professor, Department of Law, Brahmanand College, Kanpur.**
****BA-LL.B. 3rd Semester, Gautam Buddha University, Noida.**

[1] *Shreya Singhal v. Union of India*, Writ Petition (Criminal) No.167 of 2012 decided on March 24, 2015.

data by intermediary, e-commerce frauds like personation commonly known as Phishing, identity theft and offensive messages through communication services' without disclosing identity have become very easy. In such circumstances, the issue of blocking websites is more relevant and significant. The present paper unearths the legal provisions relating to blocking of websites in India with some recommendations relevant in this regard.

Understanding Blocking of Websites:

The internet websites may be of different types, nature, and ideas but one thing is common i.e. publication of information. Information may be for any particular group, for whole world or for any specific purpose which are accessible through internet connection and thus it is one mode of expression of our thoughts, ideas and opinions which are guaranteed under various international and regional instruments[2] as a fundamental human right for every person around the world. Like this, the Constitution of India also recognizes the Freedom of Speech and Expression under Article 19 (1) (a) which empowers to every Indian citizen to exercise this fundamental right without unreasonable and arbitrary restrictions. As the internet holds enormous potential for development of society, the freedom of speech and expression is not available to traditional media only rather it is available for internet and all types of emerging media platforms also. On June 29, 2012, the Human Rights Council unanimously adopted the landmark *Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet*[3] in which it has been affirmed that-

> "The same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with Articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights."

Article 19 (2) of the Constitution of India mentions the restrictions about freedom available under Article 19 (1) (a), it means that freedom of speech and expression is not absolute right and restrictions may be imposed on the grounds mentioned under Article 19 (2). Article 19 (2) mentions that 'nothing in sub-clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interests of the sovereignty and integrity of India, the security of the State,

---

[2] Article 19 of the *Universal Declaration of Human Rights;* Article 19 of the *International Covenant on Civil and Political Rights*; Article 15(3) of the *International Covenant on Economic, Social and Cultural Rights*; Article 5 of the *International Convention on the Elimination of All Forms of Racial Discrimination*; Article 12 and Article 13 of the *Convention on the Rights of the Child*; Article 13 of the *International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families*; Article 13 of the *American Convention on Human Rights*; Article 10 of the *European Convention on Human Rights*; Article 9 of the *African Charter on Human and Peoples Rights*; Article 32 of the *Arab Charter of Human Rights.*

[3] A/HRC/20/L.13 United Nations General Assembly

friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence'. Thus, it is clear that the access of internet websites may be restricted on the following grounds-

* in the interest of sovereignty and integrity of India
* security of the State
* friendly relations with foreign States
* public order
* decency or morality
* in relation to contempt of court, defamation or incitement to an offence

Thus, undoubtedly the internet websites have a lot of things for all round development of humanity but at the same time the State, being the custodian and protector of its citizens, has right to block access of websites which contain unwanted, harmful and controversial contents.

Procedure of Blocking of Websites: Blocking of websites in India may be classified in two parts: Before 2009 and after 2009.

Before 2009- Before 2009, the power to issue the instructions in the context of blocking of websites in India was vested with Computer Emergency Response Team-India (CERT-IND) under the notification.[4] In case of a complaint regarding website, the CERT-IND had to verify the authenticity of the complaint and satisfying that action of blocking of website is absolutely essential, had to instruct Department of Telecommunications, Government of India to block the website. The CERT-IND could be approached by the-

(a) Secretary, National Security Council Secretariat (NSCS).
(b) Secretary, Ministry of Home Affairs, Government of India.
(c) Foreign Secretary in the Department of External Affairs or a representative not below the rank of Joint Secretary.
(d) Secretaries, Departments of Home Affairs of each of the States and of the Union Territories.
(e) Central Bureau of Investigation (CBI), Intelligence Bureau (IB), Director General of Police of all the States and such other enforcement agencies.
(f) Secretaries of Heads of all the Information Technology Departments of all the States and Union Territories not below the rank of Joint Secretary of Central Government.
(g) Chairman of the National Human Rights Commission or Minorities Commission or Scheduled Castes or Scheduled Tribes Commission or National Women Commission.
(h) The directives of the Courts.
(i) Any others as may be specified by the Government.

The Department of Telecommunications was under duty to ensure the blocking of websites and inform CERT-IND accordingly. But, latter in this

[4] New Delhi, the 27th February, 2003, G.S.R.181(E)

respect separate legislative norms were felt very much necessary and in 2008 the Information Technology Act, 2000 was amended.

After 2009- In the Information Technology Act, 2000 the major amendments were made in the year 2008[5] and one of them is insertion of section 69A which empowers the Central Government of India to block the access of any website by public. This section provides as under-

> *69-A. Power to Issue Directions for Blocking for Public Access of Any Information through Any Computer Resource.*-(1) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.
>
> (2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.
>
> (3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

Gujarat High Court in *Gaurav Sureshbhai Vyas v. State of Gujarat and others*[6], said that "the aforesaid Section shows that the situations envisaged are, "in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above". Further, a direction can be issued under Section 69A for blockage of public access to such information and it may also be relating to "any information generated, transmitted, received, stored or posted in any computer resource".

Thus, it is clear from section 69A that the Central Government of India may direct in writing to block access of any internet websites which are violating the constitutional and statutory boundaries. Under the provisions of section 69A (2), the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 have been framed.

Constitutional Validity of Section 69A and Rules, 2009-

The constitutional validity of section 69A and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public)

---

[5] The Information Technology (Amendment) Act, 2008

[6] Writ Petition (Pil) No. 191 of 2015 decided on 15/09/2015.

Rules, 2009 was assailed before Hon'ble Supreme Court of India[7] on the following grounds-

* There is no pre-decisional hearing afforded by the Rules particularly to the "originator" of information.
* Procedural safeguards such as which are provided under Section 95 and 96 of the Code of Criminal Procedure are not available here.
* The confidentiality provision affects the fundamental rights of the petitioners.

But, the Court did not accept the plea raised as mentioned above and held that the first and foremost, blocking can only be resorted to where the Central Government is satisfied that it is necessary so to do. Secondly, such necessity is relatable only to some of the subjects set out in Article 19(2). Thirdly, reasons have to be recorded in writing in such blocking order so that they may be assailed in a writ petition under Article 226 of the Constitution. Further, the Court held that the Rules provide for a hearing before the Committee set up - which Committee then looks into whether or not it is necessary to block such information. It is only when the Committee finds that there is such a necessity that a blocking order is made. It is also clear from an examination of Rule 8 that it is not merely the intermediary who may be heard. If the "person" i.e. the originator is identified he is also to be heard before a blocking order is passed. Above all, it is only after these procedural safeguards are met that blocking orders are made and in case there is a certified copy of a court order, only then can such blocking order also be made. It is only an intermediary who finally fails to comply with the directions issued who is punishable under sub-section (3) of Section 69A. Furthermore, the Court said that merely because certain additional safeguards such as those found in Section 95 and 96 CrPC are not available does not make the Rules constitutionally infirm. Thus, the court was of the view that the Rules are not constitutionally infirm in any manner.

Responsibilities under Rules- The Rules, 2009 have prescribed the responsibilities of the following institutions in respect of blocking of websites as under-

Central Government-The Central Government of India has been expected to appoint a Designated Officer by notification in Official Gazette to an officer of the Central Government not below the rank of a Joint Secretary for the purpose of issuing direction for blocking the access by the public any information generated, transmitted, received, stored or hosted in any computer resource.[8] It is worthwhile to mention that the Rules have provided to deal with the matter through appointing a Central Government Officer not below the rank of Joint Secretary which shows the seriousness of the matter. Section 2 (1) (k) of the Act, 2000 defines the term "computer resource" as 'computer, computer system, computer network, data, computer data base or software'. The Designated Officer does not entertain any complaint or request for blocking directly from

[7] *Shreya Singhal v. Union of India*, Writ Petition (Criminal) No.167 of 2012 decided on March 24, 2015.
[8] Rule 3

any person rather it accepts request or complaint from the Nodal Officer of an Organization or from a competent court. He is under obligation to maintain complete record of the request received and action taken thereof, in electronic database and also in register of the cases of blocking for public access of the information generated, transmitted, received, stored or hosted in a computer resource.[9]

Organisations-The Rules define the term "organisation"[10] to include the following-

* Ministries or Departments of the Government of India
* State Governments and Union territories
* Any agency of the Central Government, as may be notified in the Official Gazette, by the Central Government.

These organisations have been mandated to designate one of its officers as the Nodal Officer and accordingly the same has to be intimated to the Central Government in the Department of Information Technology under the Ministry of Communications and Information Technology, Government of India in addition to the publication of the name of the said Nodal Officer on their website.[11]

Intermediaries- An "intermediary", with respect to any particular electronic message, means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.[12] The Rules mandate to every intermediary to designate at least one person to receive and handle the directions for blocking of access by the public any information generated, transmitted, received, stored or hosted in any computer resource. The Designated Person of the Intermediary shall acknowledge receipt of the directions to the Designated Officer within two hours on receipt of the direction through acknowledgement letter or fax or e-mail signed with electronic signature.

Process of Websites Blocking- The whole process of blocking of websites may be divided in the following parts-

On Application of Any Person- Where any person finds any objectionable or unwanted content in any website, he may send complaint to the “Nodal Officer” of the concerned Organization for blocking the concerned website. After receiving the complaint, the organisation has to examine the received complaint to satisfy themselves about the need for taking of action in the light of the parameters laid down in Section 69A(1) of the Act, 2000 and after being satisfied, it has to transmit the request in writing on the letter head of the respective organisation either by mail or by fax or by e-mail through its Nodal Officer to the Designated Officer in the specified format. The Designated Officer has to acknowledge the receipt of such request within a period of twenty four hours of its receipt and

---

[9] Rule 15
[10] Rule 2 (g)
[11] Rule 4
[12] Section 2 (1) (w) of the Information Technology Act, 2000.

such request has to be assigned a number alongwith the date and time of its receipt.[13]

The request made by Nodal Officer and received by the Designated Officer alongwith the printed sample content of the alleged offending information or part thereof has to be examined by a Committee consisting of the Designated Officer as its Chairperson and representatives, not below the rank of Joint Secretary in Ministries of Law and Justice, Home Affairs, Information and Broadcasting and the Indian Computer Emergency Response Team.[14] At the first hand, the Committee's whole exercise will be to identify the person/intermediary who has hosted the information or part thereof as well as the computer resource. If the concerned person/intermediary is identified, the Committee has to issue notice to appear and submit their reply and clarifications at a specified date and time, which shall not be less than forty-eight hours from the time of receipt of such notice by such person/intermediary. In case of non-appearance of such person/intermediary, who has been served with the notice, the Committee shall give specific recommendation in writing with respect to the request received from the Nodal Officer, based on the information available with the Committee. But, where such a person/intermediary is a foreign entity or body corporate as identified by the Designated Officer, notice shall be sent by way of letters or fax or e-mail signed with electronic signatures to such foreign entity or body corporate and any such foreign entity or body corporate shall respond to such a notice within the time specified therein, failing which the Committee shall give specific recommendation in writing with respect to the request received from the Nodal Officer, based on the information available with the Committee.[15]

If the Committee finds that the request is covered under section 69A (1) and it is justifiable to block requested website, the Designated Officer shall submit the recommendation of the Committee to the Secretary in the Department of Information Technology under the Ministry of Communications and Information Technology, Government of India for his approval. If the recommendation is approved by the Secretary, Department of Information Technology, he will direct the concerned agency of the Government or the intermediary to block the offending information generated, transmitted, received, stored or hosted in their computer resource for public access within the time limit specified in the direction but if the recommendation is not approved by the Secretary, the Designated Officer shall convey the same to such Nodal Officer.

In Emergency Cases- When the Designated Officer receives any request which is of emergency nature where delay is not acceptable, he has to examine the request and printed sample information and consider whether the request is within the scope of section 69A (1) and it is necessary or expedient and justifiable to block such information or part thereof and submit the request with specific recommendations in writing to Secretary, Department of Information Technology. Thereafter, the Secretary, Department of Information Technology

---

[13] Rule 6
[14] Rule 7
[15] Rule 8

may, if he is satisfied that it is necessary or expedient and justifiable for blocking for public access of any information or part thereof through any computer resource and after recording reasons in writing, as an interim measure issue such directions as he may consider necessary to such identified or identifiable persons or intermediary in control of such computer resource hosting such information or part thereof without giving him an opportunity of hearing. The Designated Officer, at the earliest but not later than forty-eight hours of issue of direction, shall bring the request before the Committee for its consideration and recommendation. On receipt of recommendations of Committee, Secretary, Department of Information Technology, shall pass the final order as regard to approval of such request and in case the request for blocking is not approved by the Secretary, Department of Information Technology in his final order, the interim direction issued shall be revoked and the person or intermediary shall be accordingly directed to unblock the information for public access.[16]

The Rules mandate to decide the request received from the Nodal Officer expeditiously and in any case it should not be more than seven working days from the date of receipt of the request.[17]

On Court's Order- When the Designated Officer receives the certified copy of the order of a competent court to block of any information or part thereof of website, he shall immediately submit it to the Secretary, Department of Information Technology and initiate action as directed by the court.[18]

Non-Compliance by Intermediary- If the intermediary does not comply with the direction of the Central Government, the punishment may be awarded with imprisonment for a term which may extend to seven years with fine.[19] In this respect it is necessary to mention here that in case of failure on the part of intermediary to comply with the direction issued to him, the Designated Officer shall, with the prior approval of the Secretary, Department of Information Technology, initiate appropriate action as may be required to comply with the provisions of section 69A (3) of the Act.[20]

The Rules provide that strict confidentiality shall be maintained regarding all the requests and complaints received and actions taken thereof.[21]

Delhi High Court in *UTV Software Communication Ltd. v. 1337X.TO*[22], expressed its views that since website blocking is a cumbersome exercise and majority of the viewers / subscribers who access, view and download infringing content are youngsters who do not have knowledge that the said content is infringing and / or pirated, it directed the MEITY/DOT to explore the possibility

---

[16] Rule 9
[17] Rule 11
[18] Rule 10
[19] Sec. 69A(3) of the Act, 2000
[20] Rule 12
[21] Rule 16
[22] CS(COMM) 768/2018 decided on 10 April, 2019

of framing a policy under which a warning is issued to the viewers of the infringing content, if technologically feasible in the form of e-mails, or pop-ups or such other modes cautioning the viewers to cease viewing/downloading the infringing material. In the event the warning is not heeded to and the viewers / subscribers continue to view, access or download the infringing/pirated content, then a fine could be levied on the viewers/subscribers.

Conclusion:

The contribution of information technology is significant for each and every individual in present scenario through removing the geographical boundaries etc. The people are exercising their freedom of speech and expression in varied ways with the help of computer, mobile phones and internet. In line with the Rules and laws, the Department of Telecommunications, Ministry of Communication & IT, Government of India issued a letter, blocking 857 internet websites, under the provision of section 79 (3) (b) of the Information Technology Act, 2000 as the content hosted in these websites relate to morality, decency as given in Article 19 (2) of the Constitution of India.[23] But the material fact is that if these websites are blocked again many websites are being launched without any control. To deal with such issues, the international cooperation is required in which the separate laws of distinct sovereign countries are a great barrier. More than this, only notifying by Government of India cannot solve the problem rather continuous monitoring is required and if any intermediary/internet service provider is found guilty of violating these norms, there should be huge amount of fine in addition to imprisonment having deterrent effects. What can be expected from private sector internet service providers whose single motto is to get benefit, the condition of Government owned BSNL is also fully dissatisfactory. Despite the ban imposed by Government of India as mentioned above, the BSNL has allowed to access many banned websites.

***

[23] No. 813-7/25/2011-DS (Vol.-V) dtd. 31.07.2015